

Quantum Information Science

An abstract painting featuring vibrant, swirling colors like purple, yellow, blue, and red. The composition includes several circular, vortex-like patterns and two stylized faces in profile, facing each other. The overall style is expressive and dynamic, with visible brushstrokes.

Chris
Monroe

University of Maryland
Department of Physics

iqi JOINT
QUANTUM
INSTITUTE

National Institute of
Standards and Technology

Boris
2005

The Integrator

Robert Noyce dreamed up the microchip in a 1959 notebook entry.

BY ROGER LOWENSTEIN

THE REVELATORY MOMENT of the electronics age arguably came in January 1959, when Robert Noyce, an engineer and a founder of Fairchild Semiconductor, scrawled in his notebook the words "Methods of Isolating Multiple Devices." Under that obscure heading, Noyce went on to write, "In many applications now it would be desirable to make multiple devices on a single piece of silicon in order to be able to make interconnections between devices as part of the manufacturing process, and thus reduce size, weight, etc., as well as cost per active element."

Although the word for it did not yet exist, Noyce was describing the microchip. A former protégé of William Shockley, the coinventor of the transistor, Noyce understood the transformative potential of new technology as well as anyone alive.

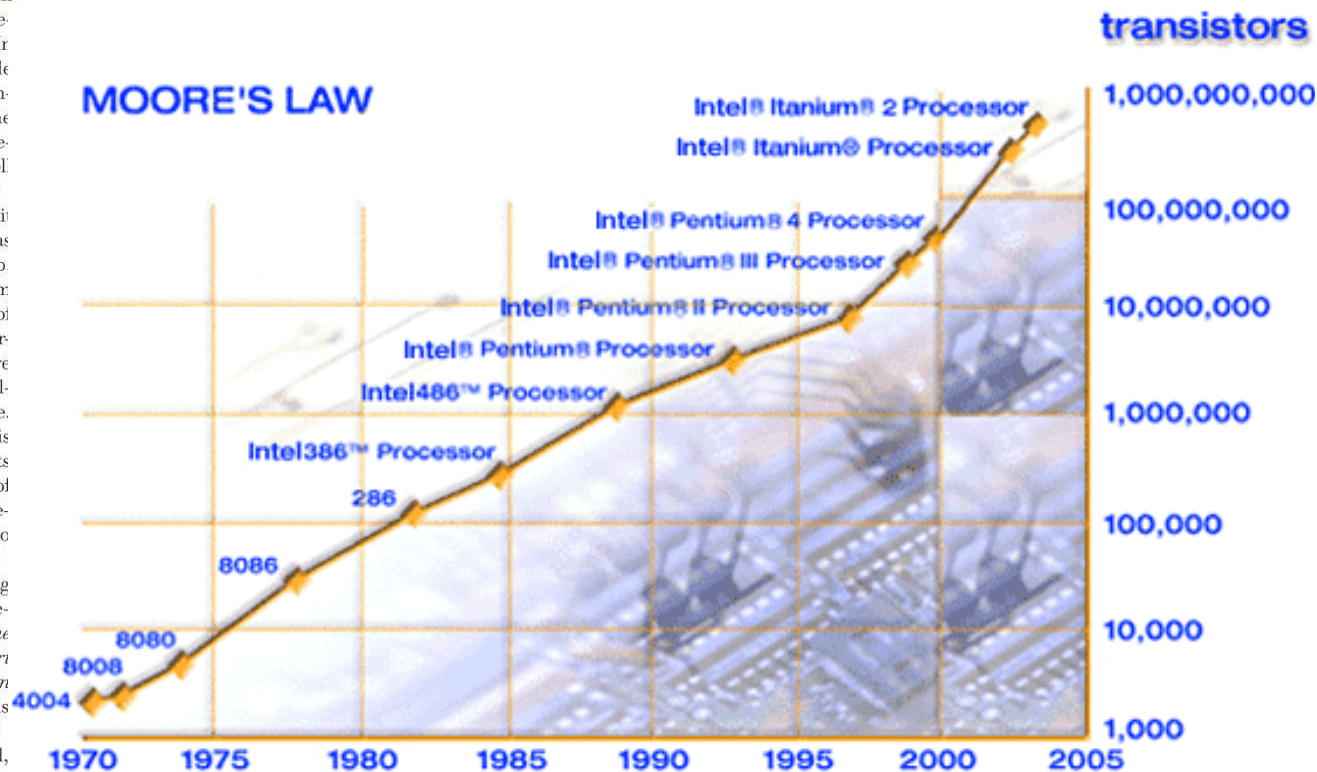
His halting follow-up on his initial idea therefore casts light not just on the history of computers but on the often befogged pathways that lead to scientific advancement.

As Leslie Berlin, a visiting scholar at Stanford University, relates in her new biography, *The Man behind the Microchip: Robert Noyce and the Invention of Silicon Valley*, "After noting his ideas in his lab notebook, Noyce did...nothing."

Fairchild was a new company, and, as Noyce later recalled, he was preoccupied with selling transistors, not with inventions "that might make you some money somewhere down the road." Noyce did not "invent" the chip to create something new but to solve an existing problem in an industrial process.

The problem was that circuits consisted of numerous discrete components (transistors, resistors, and so

MOORE'S LAW



Source: Intel

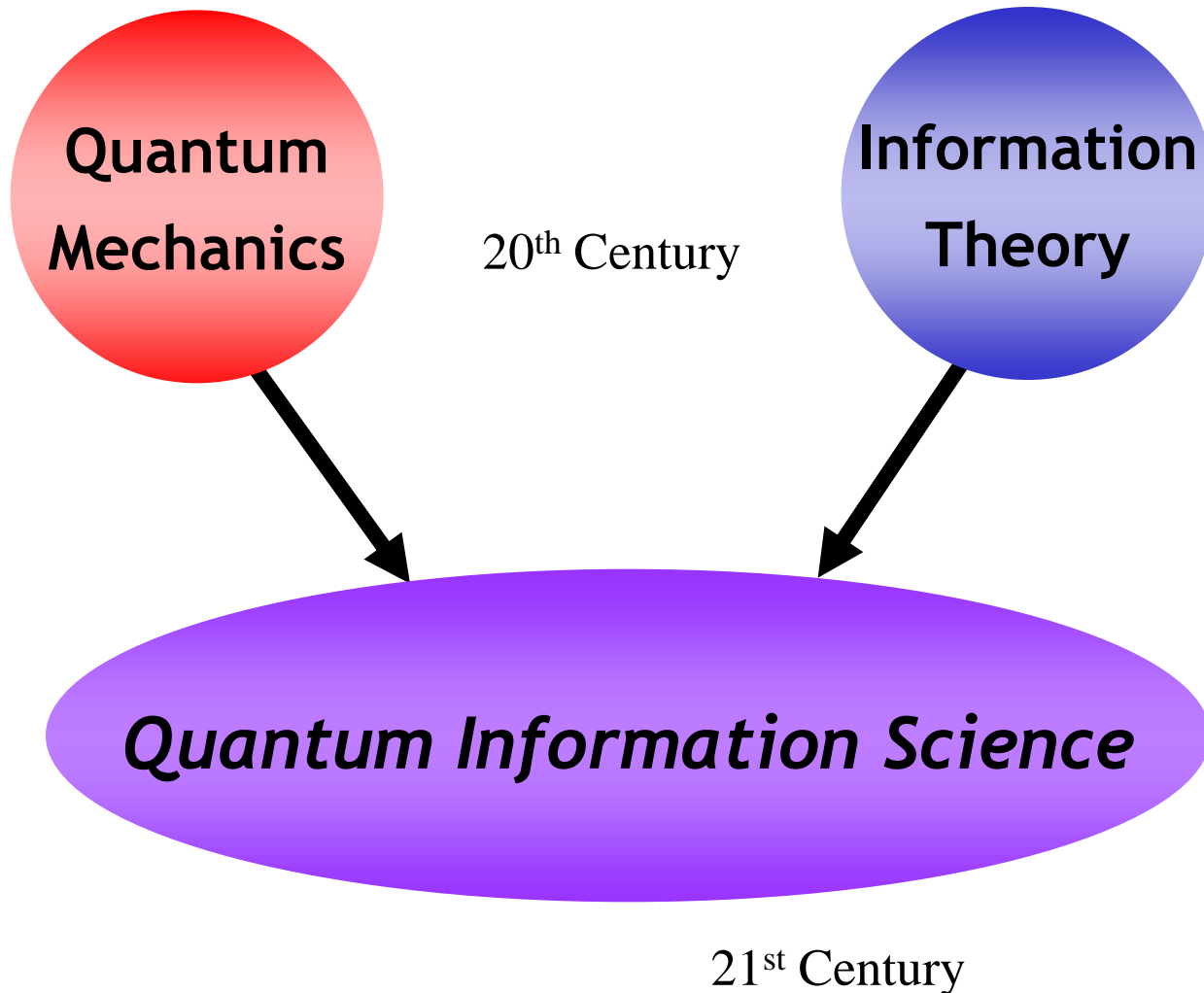
*“There's Plenty of Room at the Bottom”
(1959)*



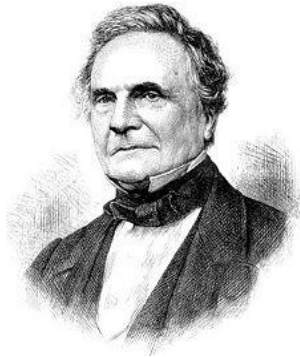
Richard Feynman

“When we get to the very, very small world – say circuits of seven atoms - we have a lot of new things that would happen that represent completely new opportunities for design. ***Atoms on a small scale behave like nothing on a large scale, for they satisfy the laws of quantum mechanics...***”

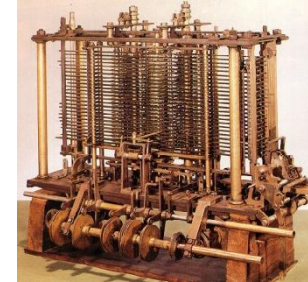
A new science for the 21st Century?



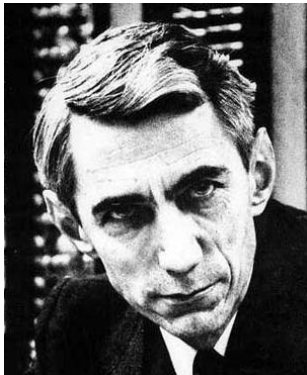
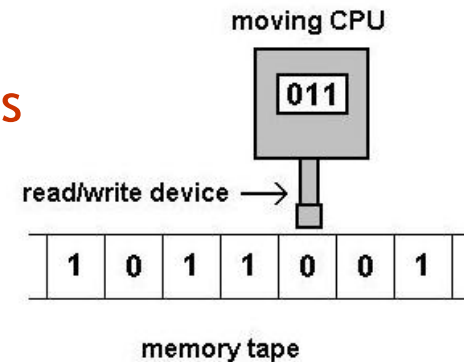
Computer Science and Information Theory



Charles Babbage (1791-1871)
mechanical difference engine



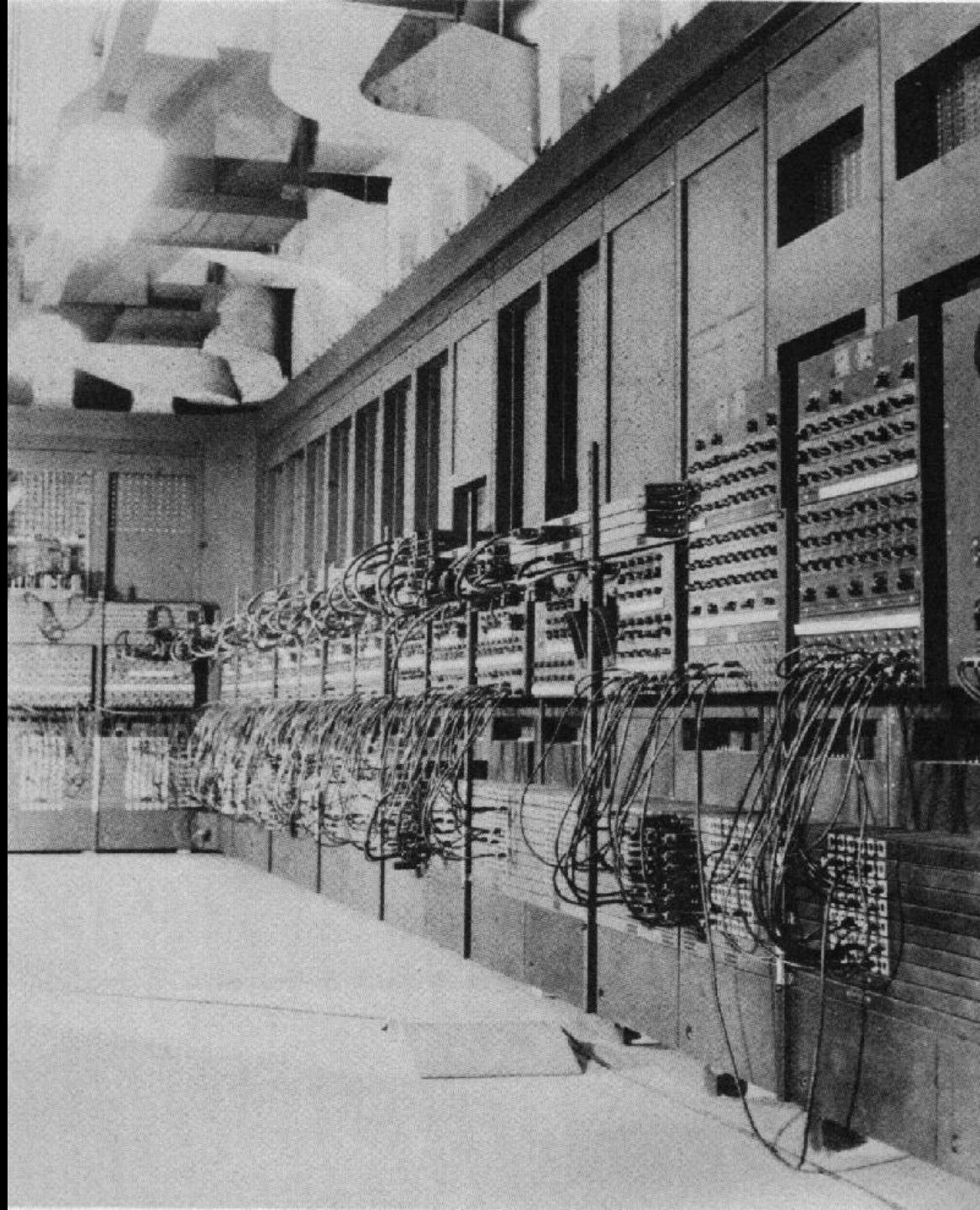
Alan Turing (1912-1954)
universal computing machines

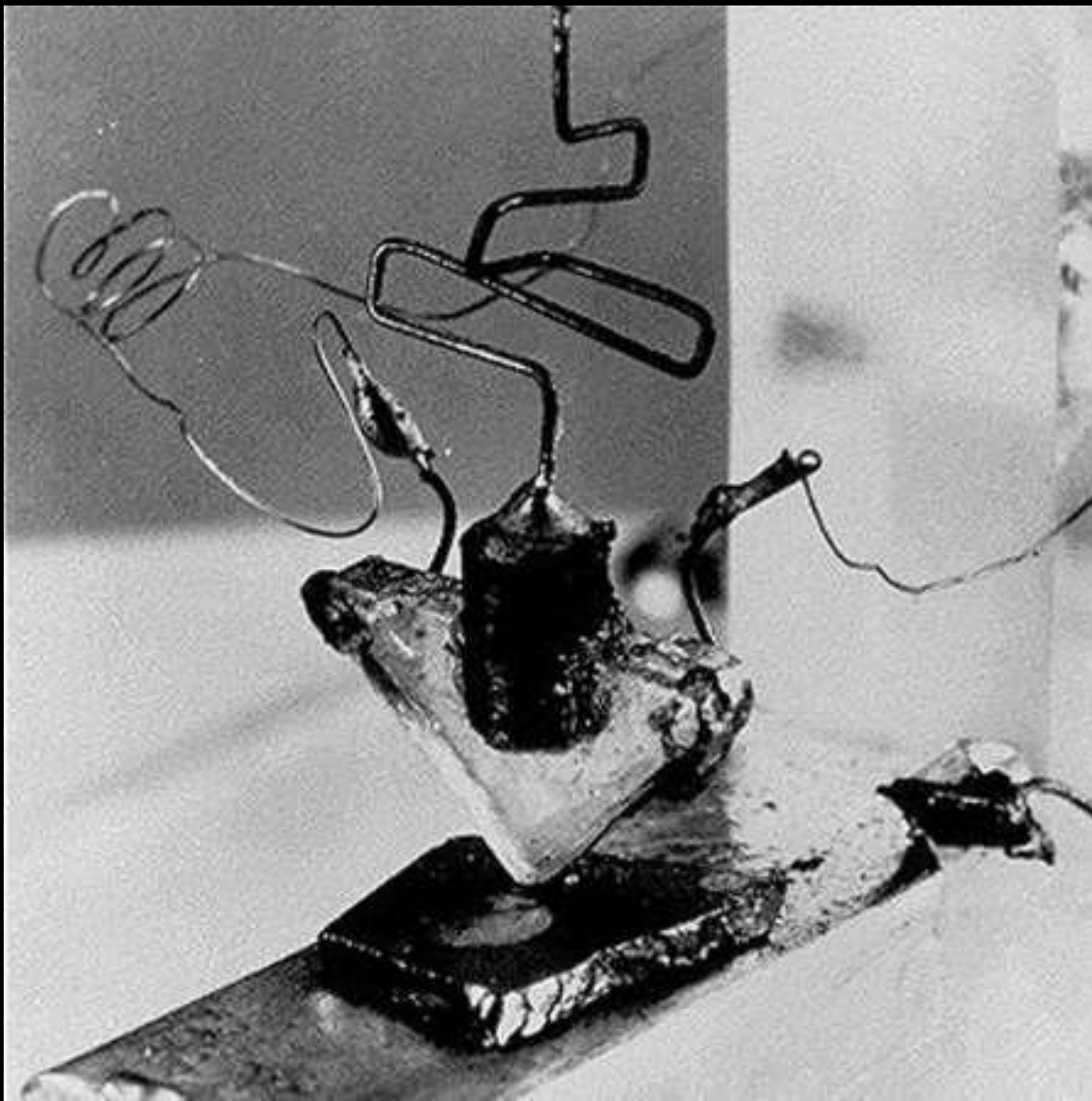


Claude Shannon (1916-2001)
quantify information: the bit

$$H = -\sum_{i=1}^k p_i \log_2 p_i$$

ENIAC (1946)





The first solid-state transistor
(Bardeen, Brattain & Shockley, 1947)

Quantum Mechanics: A 20th century revolution in physics

- Why doesn't the electron collapse onto the nucleus of an atom?
- Why are there thermodynamic anomalies in materials at low temperature?
- Why is light emitted at discrete colors?
-



Albert Einstein (1879-1955)



Werner Heisenberg (1901-1976)

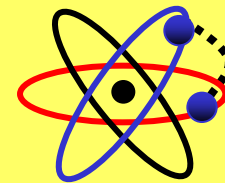


Erwin Schrödinger (1887-1961)

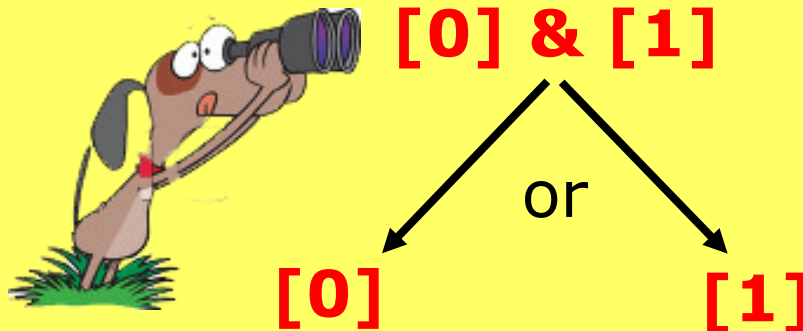
THE GOLDEN RULES OF QUANTUM MECHANICS

1. Quantum objects are waves and can be in states of superposition.

"qubit": **[0] & [1]**



2. Rule #1 holds as long as you don't look!



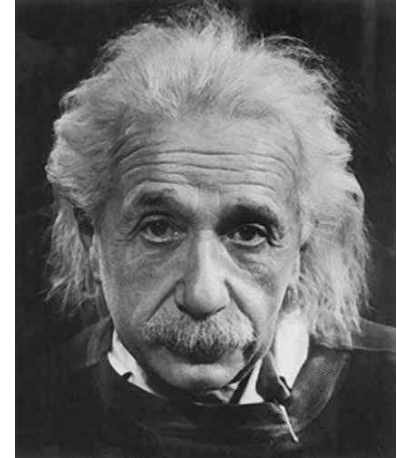
Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?

A. EINSTEIN, B. PODOLSKY AND N. ROSEN, *Institute for Advanced Study, Princeton, New Jersey*

(Received March 25, 1935)

In a complete theory there is an element corresponding to each element of reality. A sufficient condition for the reality of a physical quantity is the possibility of predicting it with certainty, without disturbing the system. In quantum mechanics in the case of two physical quantities described by non-commuting operators, the knowledge of one precludes the knowledge of the other. Then either (1) the description of reality given by the wave function in

quantum mechanics is not complete or (2) these two quantities cannot have simultaneous reality. Consideration of the problem of making predictions concerning a system on the basis of measurements made on another system that had previously interacted with it leads to the result that if (1) is false then (2) is also false. One is thus led to conclude that the description of reality as given by a wave function is not complete.



Quantum State: [0][0] & [1][1]

Entanglement: Quantum Coins

Two coins in a
quantum
superposition

[H][H] & [T][T]

1



1



Entanglement: Quantum Coins

Two coins in a
quantum
superposition

[H][H] & [T][T]

1
0



1
0



Entanglement: Quantum Coins

Two coins in a
quantum
superposition

[H][H] & [T][T]

1
0
0



1
0
0



Entanglement: Quantum Coins

Two coins in a
quantum
superposition

[H][H] & [T][T]

1
0
0
1



1
0
0
1



Entanglement: Quantum Coins

Two coins in a
quantum
superposition

[H][H] & [T][T]

1
0
0
1
1



1
0
0
1
1



Entanglement: Quantum Coins

Two coins in a
quantum
superposition

[H][H] & [T][T]

1
0
0
1
1
1



1
0
0
1
1
1



Entanglement: Quantum Coins

Two coins in a
quantum
superposition

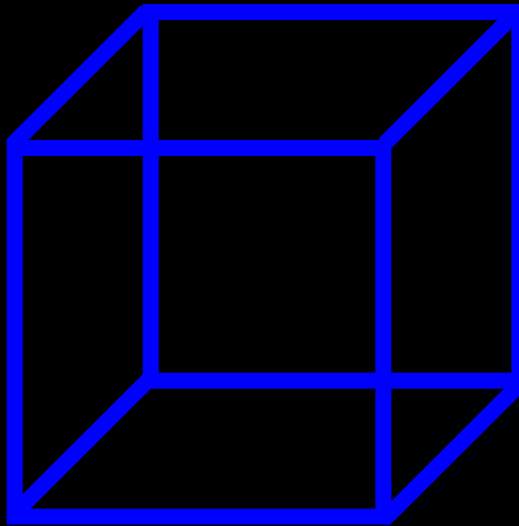
[H][H] & [T][T]

1
0
0
1
1
1
0
.
.
.



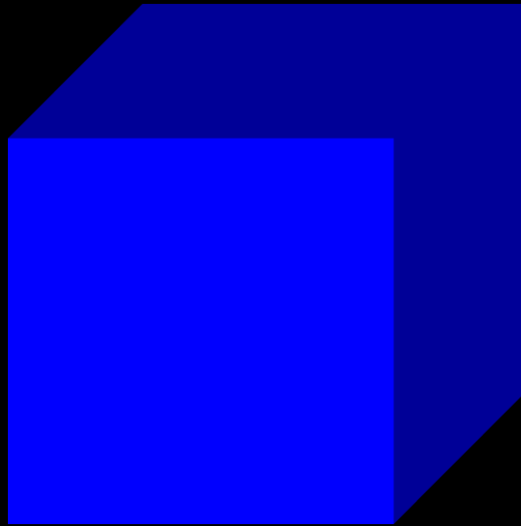
1
0
0
1
1
1
0
.
.
.

Quantum Superposition



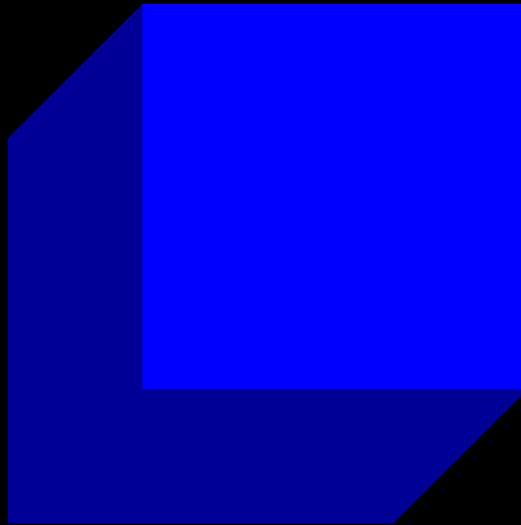
From Taking the Quantum Leap, by Fred Alan Wolf

Quantum Superposition



From Taking the Quantum Leap, by Fred Alan Wolf

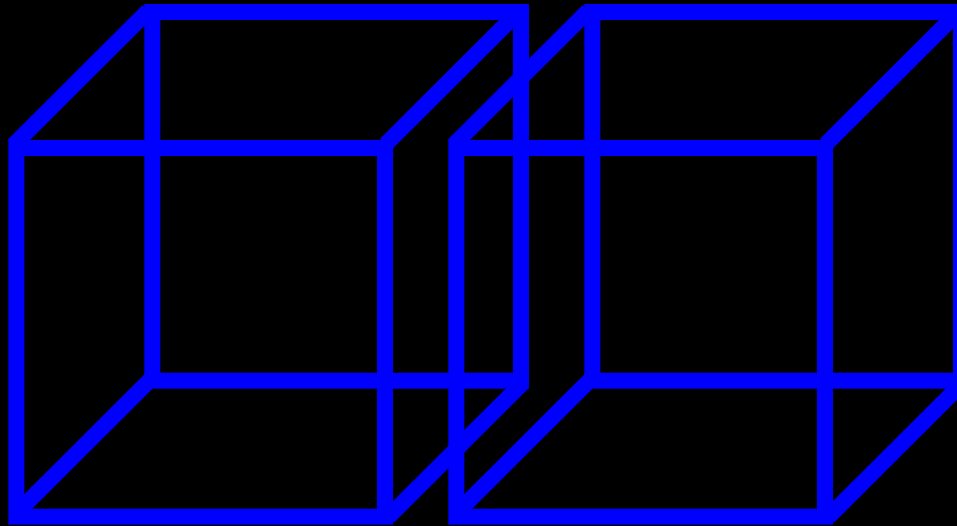
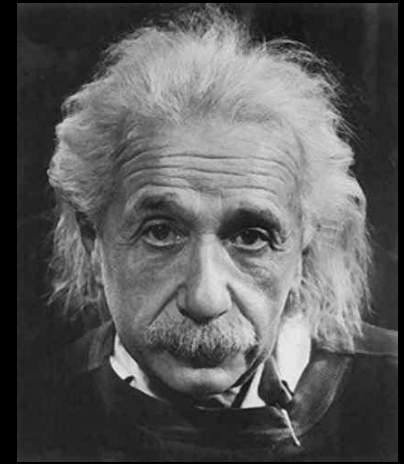
Quantum Superposition



From Taking the Quantum Leap, by Fred Alan Wolf

Quantum Entanglement

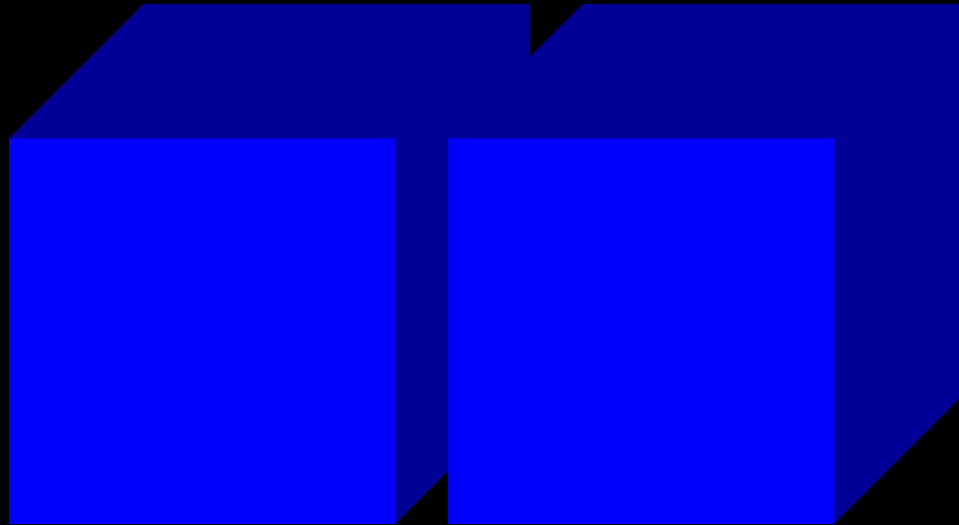
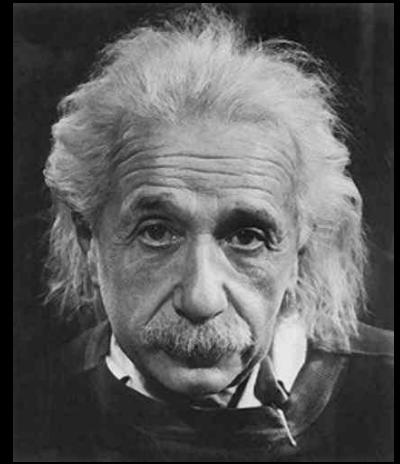
“Spooky action-at-a-distance”
(A. Einstein)



From Taking the Quantum Leap, by Fred Alan Wolf

Quantum Entanglement

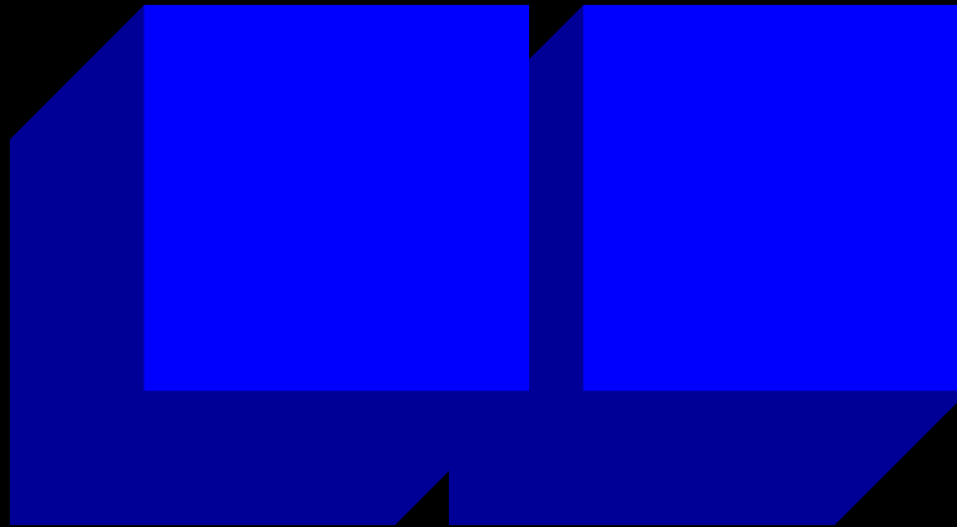
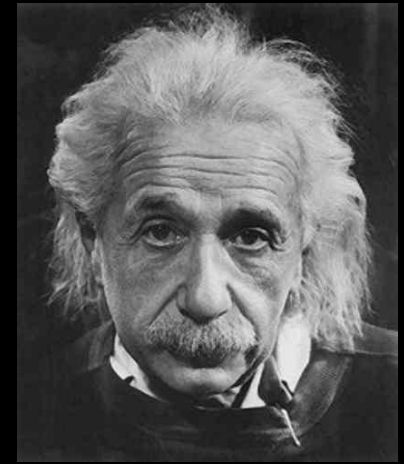
“Spooky action-at-a-distance”
(A. Einstein)



From Taking the Quantum Leap, by Fred Alan Wolf

Quantum Entanglement

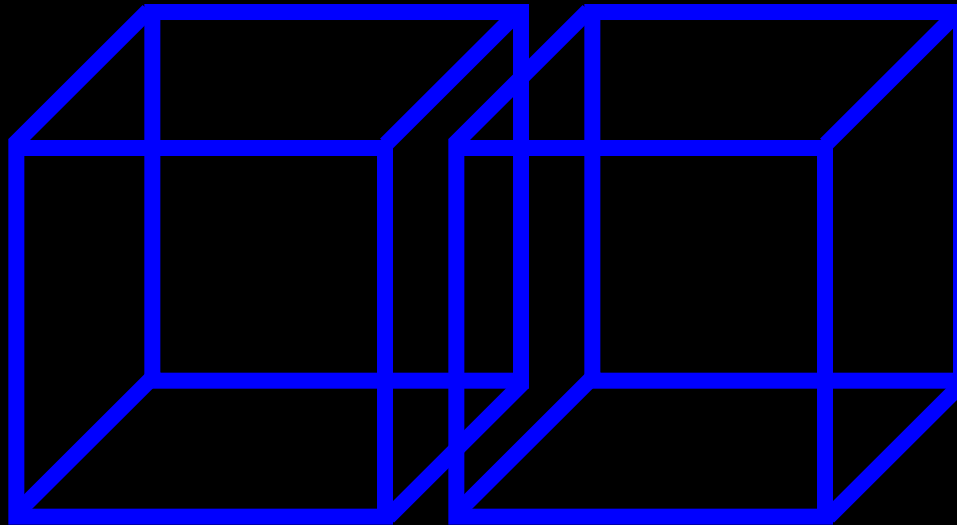
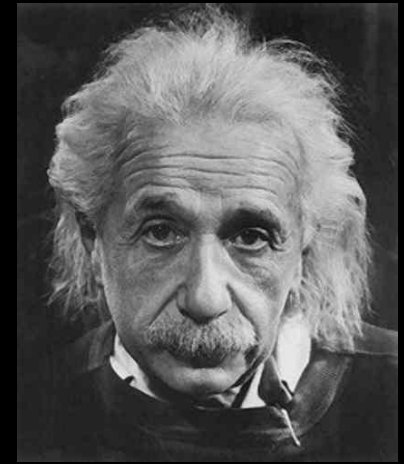
“Spooky action-at-a-distance”
(A. Einstein)



From Taking the Quantum Leap, by Fred Alan Wolf

Quantum Entanglement

“Spooky action-at-a-distance”
(A. Einstein)



From Taking the Quantum Leap, by Fred Alan Wolf



David Deutsch

“When a quantum measurement is made, the universe bifurcates!”

- Many Universes
- Multiverse
- Many Worlds

THE QUANTUM SOCIETY

*Mind, Physics, and a
New Social Vision*

DANAH ZOHAR
& IAN MARSHALL

William Morrow and Company, Inc. • New York

both aspects of some larger whole that naturally keeps them in synchrony. For Einstein, this made no sense. In his Theory of Hidden Variables, he said that there must be some mysterious common factor which accounted for all the similarities. In the analogy of the twins, this might be our shared genetic material. The controversy wore on for years, but was eventually settled by Irish physicist John Bell. His theorem—Bell's Theorem—led to experiments that finally settled the matter.

✓ If we applied Bell's Theorem to my twin and myself, we would look for some instantaneous correlation in our lives that couldn't possibly be accounted for by genetics. Imagine, for example, that I decide to enroll in a dance class in Oxford. My twin, too, might be observed to enroll in such a class in New York, at exactly the same time. Strange, but perhaps not absolutely outside some genetic predisposition linked with coincidence.

But supposing that I am observed to raise one or the other of my arms during the exercises. What does my twin do? If quantum physics is right, and important aspects of our lives are indeed instantaneously correlated, she should raise one of her arms (the opposite one) at exactly the same moment. If Einstein is right, my raising an arm should make no difference to what she does—no shared genetic material can account for simultaneous arm raising, and no faster-than-light signal can travel from Oxford to New York to tell my twin what I have done.

In fact, if we are quantum twins, every time I am seen to raise my right arm, my twin raises her left one. If I raise my left arm, she raises her right one, at exactly the same moment. Which arm I raise at any time is completely indeterminate—both my twin and I are fully ambidextrous. Each of us chooses freely which arm to raise in the dance. And yet our behavior is linked as though we are standing in the same room and there are springs connecting our arms. Instantaneous, nonlocal correlations may be “ghostly and absurd,” but they are a fact of quantum reality.

✓ In social reality, too, there often seems to be an eerie correlation between apparently separate events or situations—the spontaneous appearance of revolutions or the acceptance of new practices all over the globe, or the almost simultaneous discovery of creative ideas by two or more people working in ignorance of

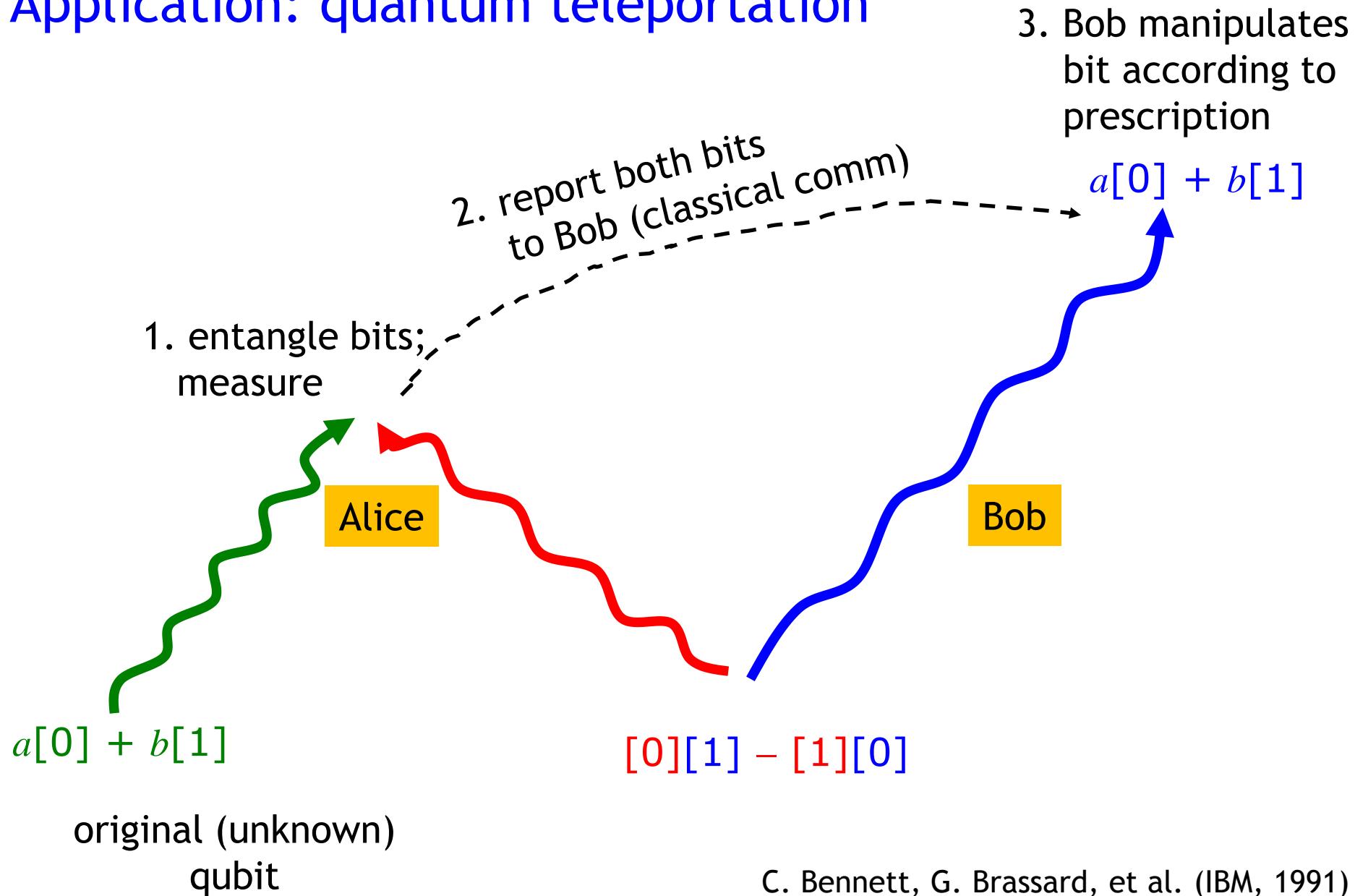
Application: quantum cryptographic key distribution

$$\begin{array}{rcl} 01011100 & \text{plaintext} & \\ + 11001010 & \text{KEY} & \\ \hline 10010110 & \text{ciphertext} & \end{array}$$



$$\begin{array}{rcl} \text{ciphertext} & 10010110 & \\ \text{KEY} & + 11001010 & \\ \hline \text{plaintext} & 01011100 & \end{array}$$

Application: quantum teleportation



Application: quantum computing

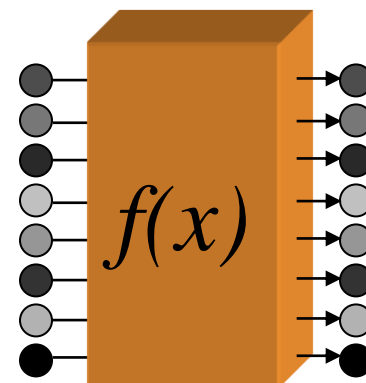
GOOD NEWS...

quantum parallel processing on 2^N inputs

Example: $N=3$ qubits

$$\Psi = a_0 [000] + a_1 [001] + a_2 [010] + a_3 [011] \\ a_4 [100] + a_5 [101] + a_6 [110] + a_7 [111]$$

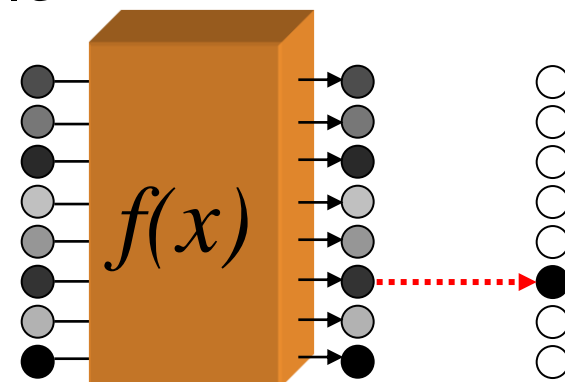
$N = 300$ qubits: $2^{300} \sim 10^{90}$ states
...more than # particles in universe!



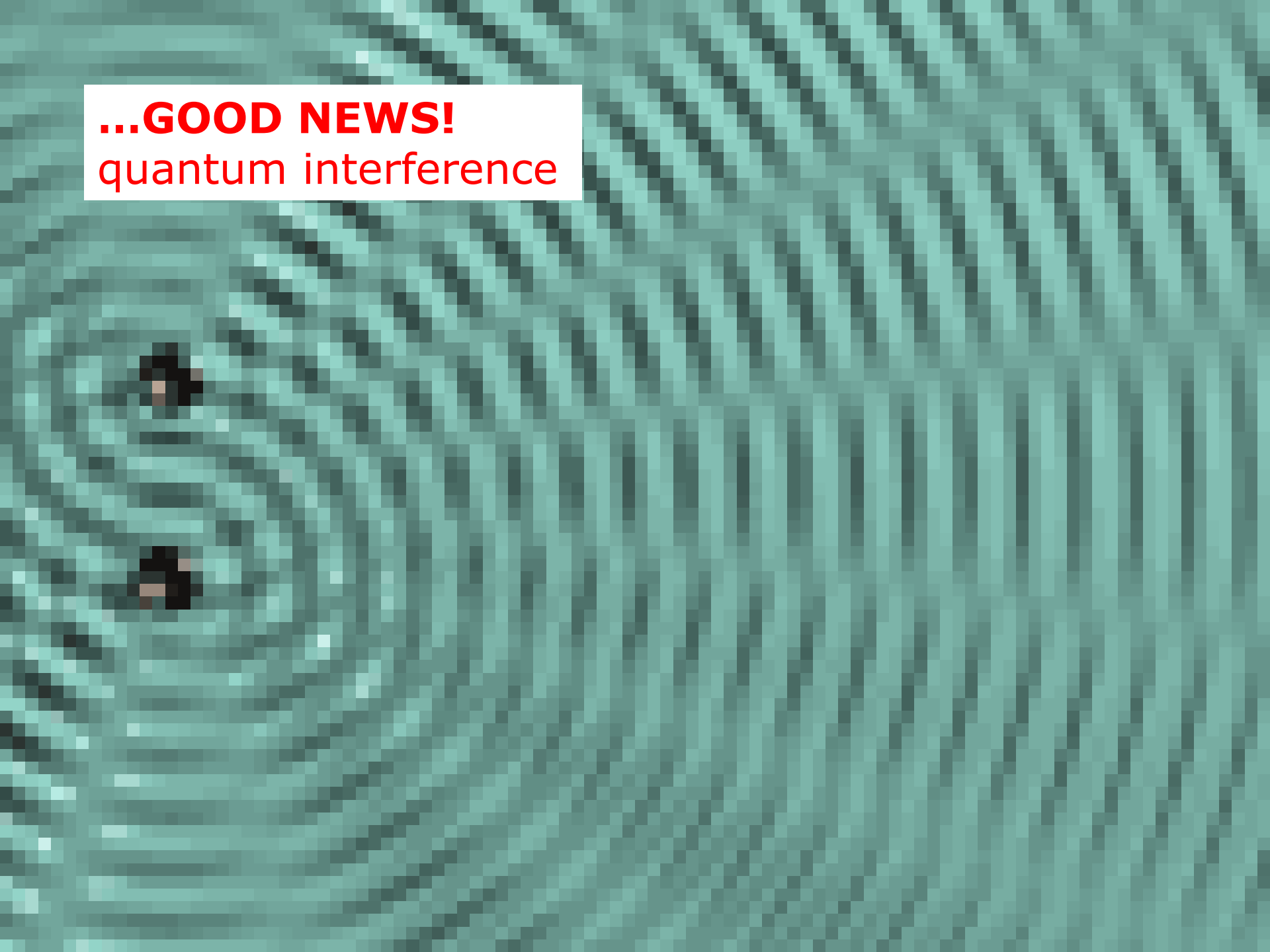
...BAD NEWS...

Measurement gives random result

e.g., $\Psi \Rightarrow [101]$

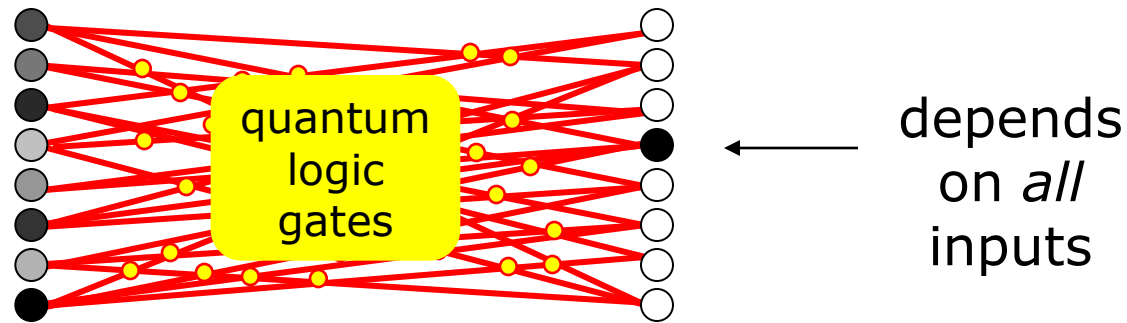


...GOOD NEWS!
quantum interference



...GOOD NEWS!

quantum interference



Deutsch (1985)

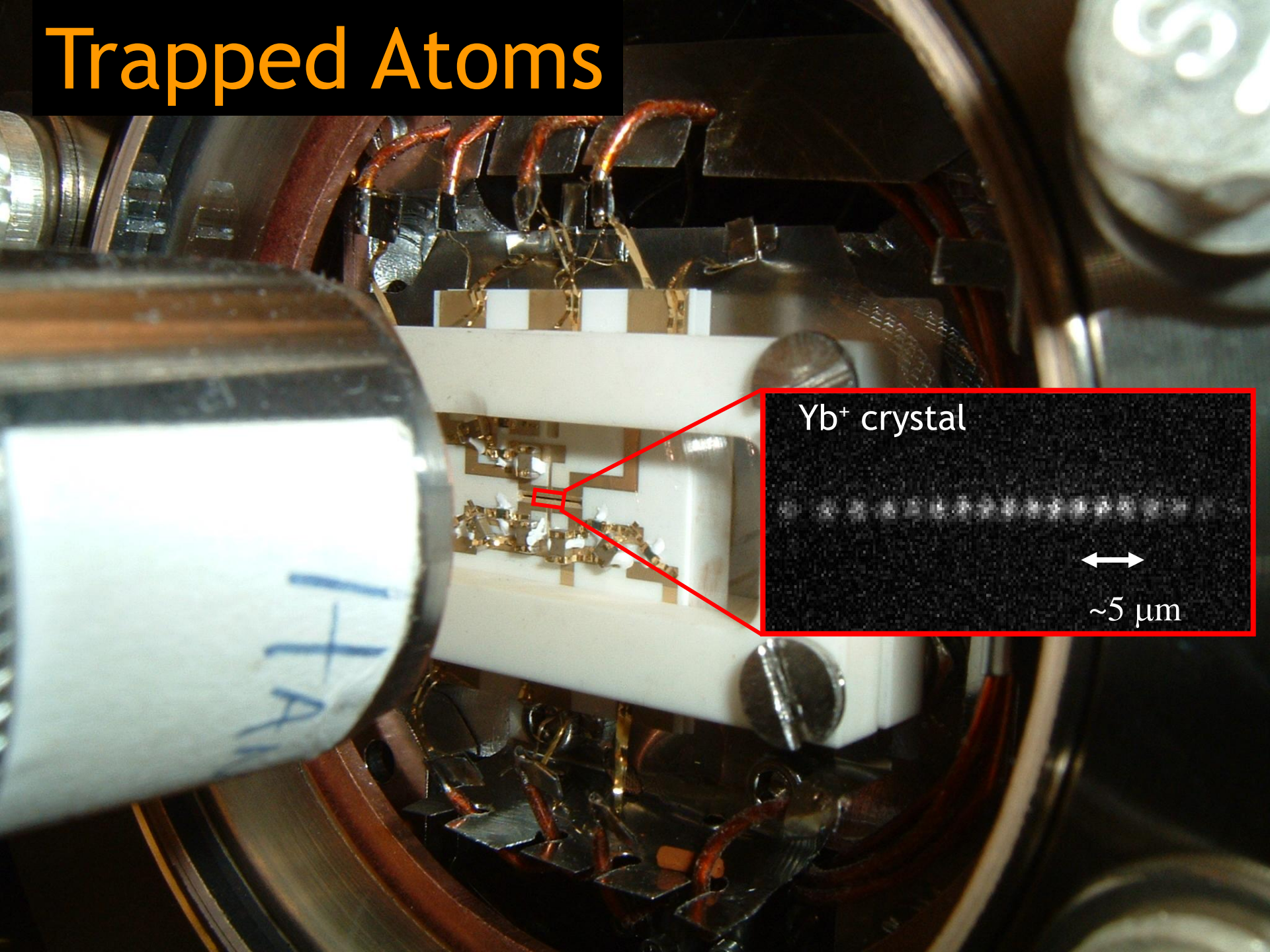
Shor (1994) fast number factoring $N = p \times q$

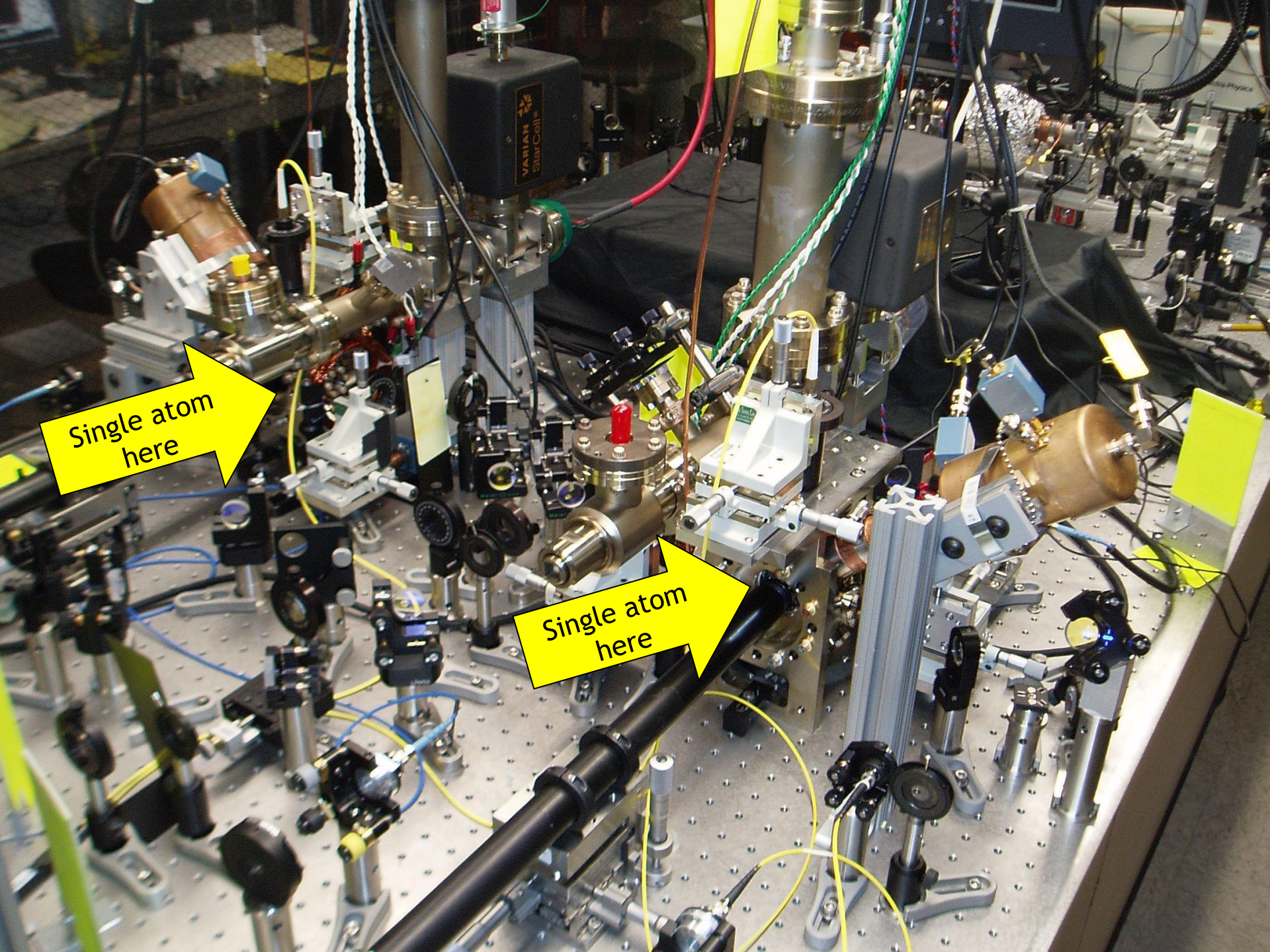
Grover (1996) fast database search

I'VE INVENTED A QUANTUM
COMPUTER, CAPABLE OF
INTERACTING WITH MATTER
FROM OTHER UNIVERSES
TO SOLVE COMPLEX
EQUATIONS.



Trapped Atoms



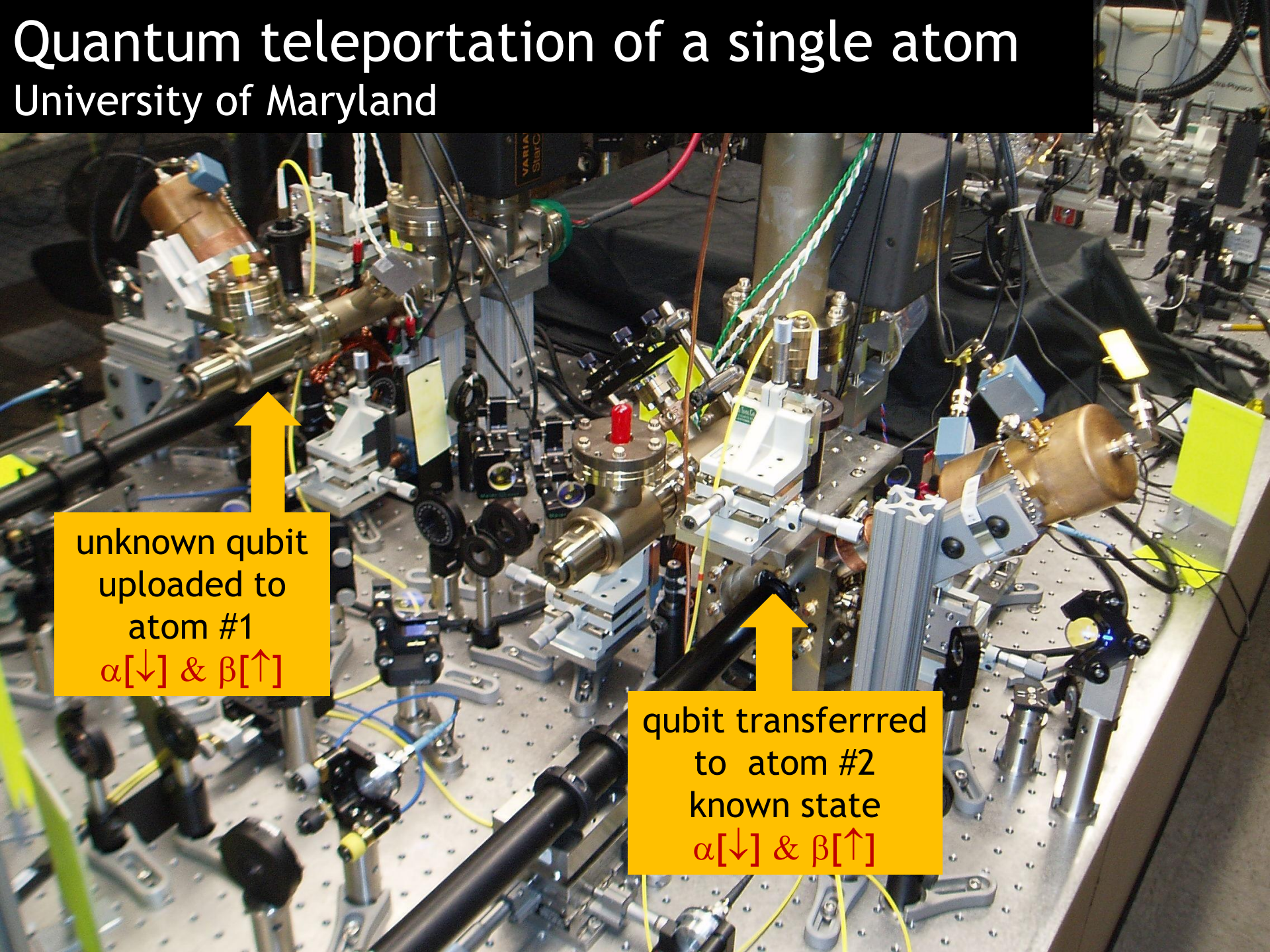


Single atom
here

Single atom
here

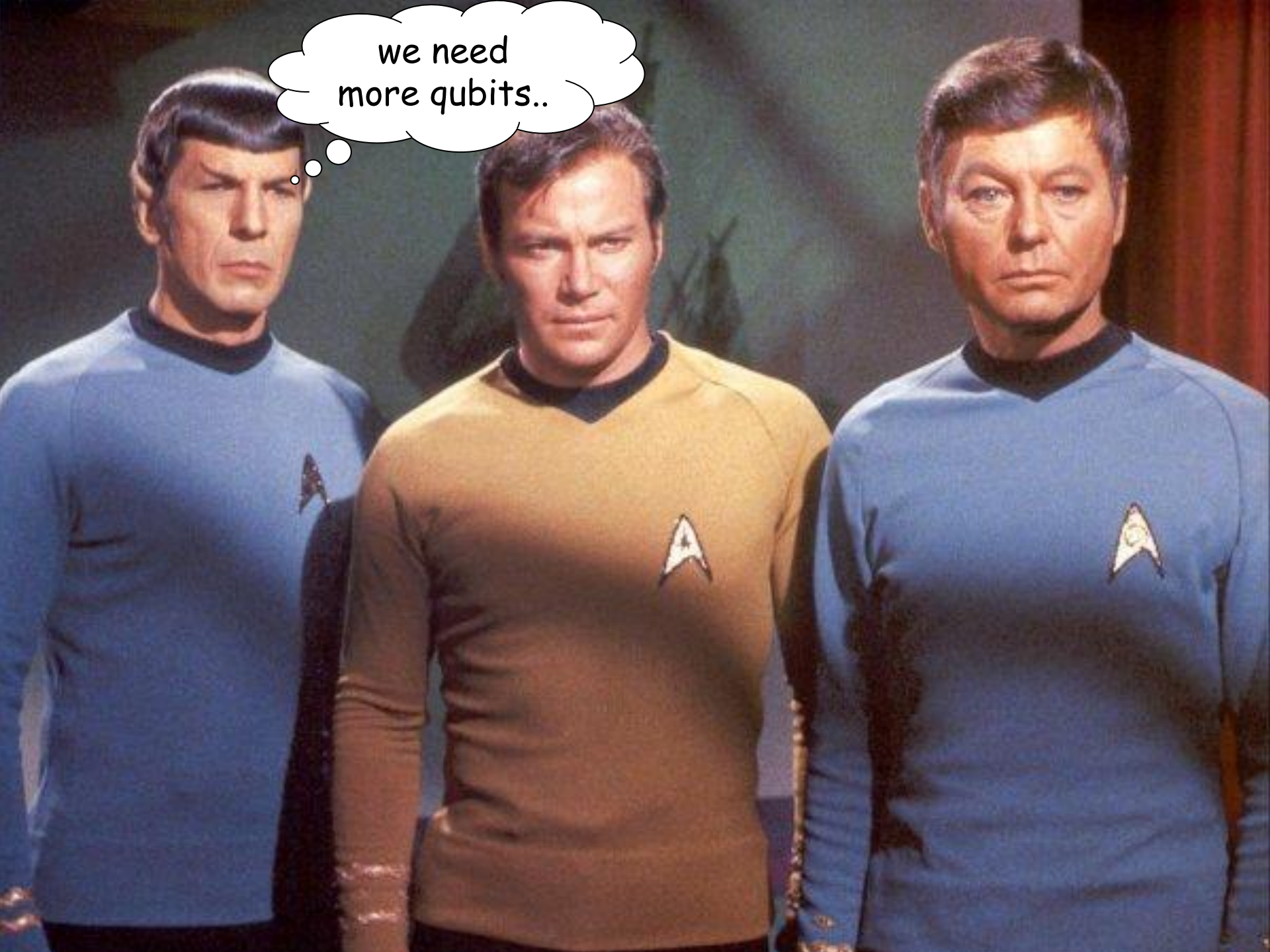
Quantum teleportation of a single atom

University of Maryland



unknown qubit
uploaded to
atom #1
 $\alpha[\downarrow]$ & $\beta[\uparrow]$

qubit transferred
to atom #2
known state
 $\alpha[\downarrow]$ & $\beta[\uparrow]$

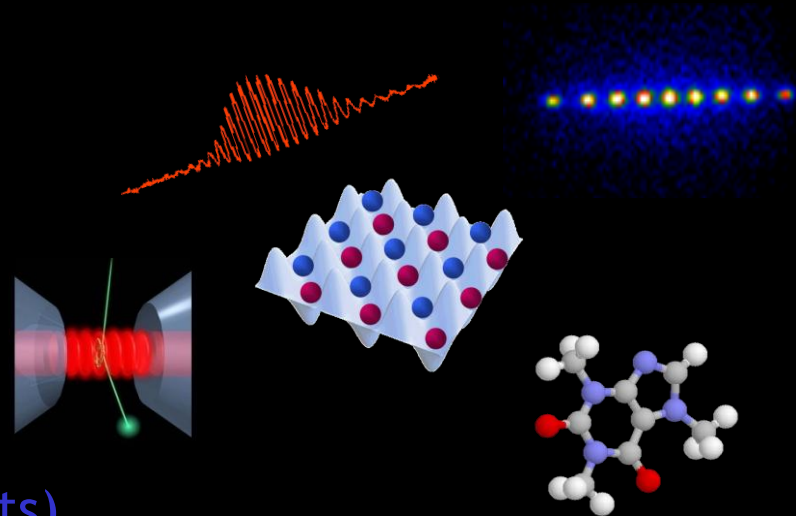
A photograph of three men in Star Trek uniforms. From left to right: Spock in a blue uniform, a man in a yellow uniform, and Kirk in a blue uniform. A thought bubble originates from Spock's head, containing the text "we need more qubits..".

we need
more qubits..

Quantum Computer Physical Implementations

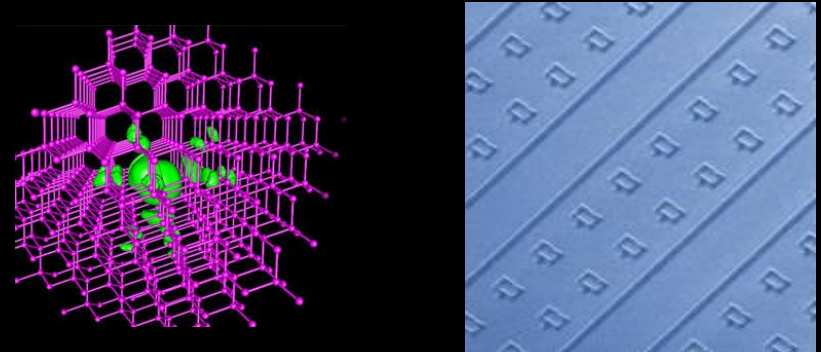
Individual atoms and photons

ion traps
atoms in optical lattices
cavity-QED



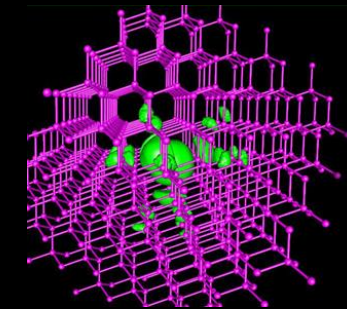
Superconductors

Cooper-pair boxes (charge qubits)
rf-SQUIDS (flux qubits)



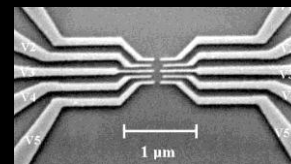
Semiconductors

quantum dots
single dopants in silicon

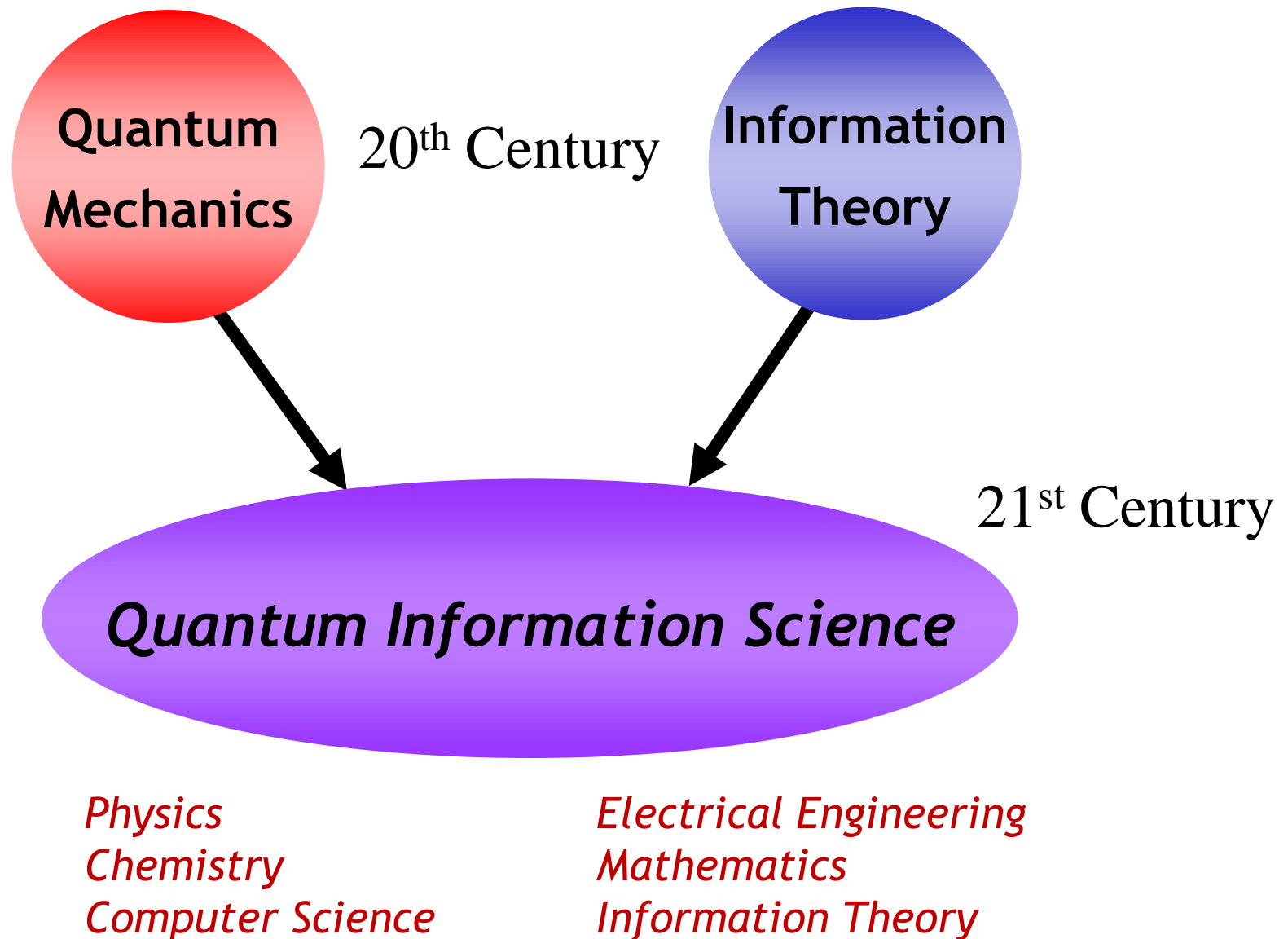


Other...

micromechanical oscillators
electrons on liquid He



A new science for the 21st Century?

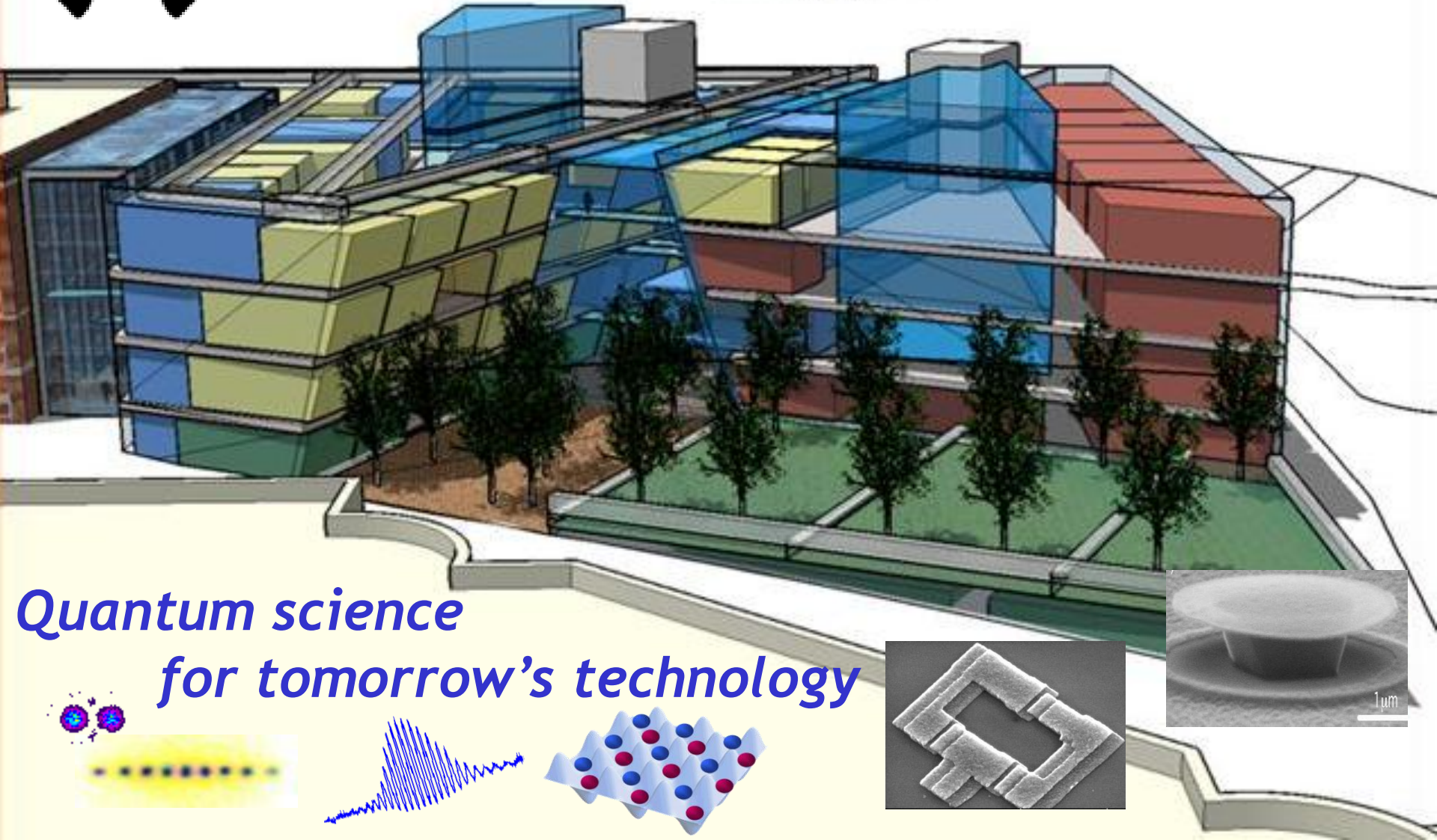




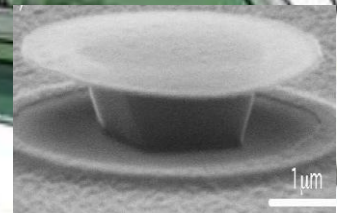
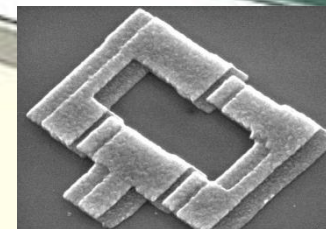
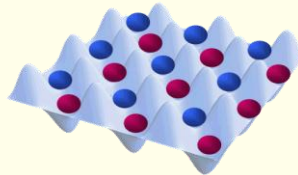
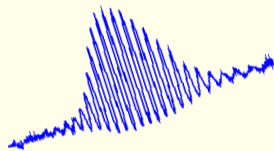
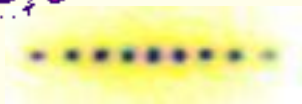
JOINT
QUANTUM
INSTITUTE



NIST



*Quantum science
for tomorrow's technology*



MagiQ

Any sufficiently advanced technology is indistinguishable from magic
– Arthur C. Clarke

MagiQ Technologies Inc. of Cambridge, Mass., refreshes its quantum keys as often as 100 times a second during a transmission, making it extremely hard to break. It sells its technology to banks and companies. Dr. Gisin is a founder of ID Quantique SA in Switzerland. The company's similar encryption tool is used by online lottery and poker firms to safely communicate winning numbers and winning hands. Votes cast in a recent Swiss federal election were sent in a similar way.

Because of its bizarre implications, quantum theory has been used to investigate everything from free will and the paranormal to the enigma of consciousness. Several serious physicists



QUANTUM RANDOM NUMBER GENERATOR USED IN GENEVA'S INTERNET VOTING OPERATION

SEPTEMBER 28, 2009

“One citizen - one vote” is the central axiom of democracy. To guarantee this in the cyberworld, the State of Geneva relies on a quantum random number generator built by ID Quantique to produce unique identifiers guaranteeing the voters’ anonymity and the vote security. This innovative solution was offered last weekend to 60’000 citizens who had the possibility to cast their vote over the Internet in the framework of the 12th official online ballot in Geneva.

D-Wave sells first quantum computer

Posted on Jun 1st 2011 by **Emma Woollacott**

Canada's D-Wave Systems has won a ringing endorsement of its controversial quantum computer - an order from Lockheed Martin. For years, D-Wave has claimed to have developed a functioning quantum computer, and for years its claims have been challenged. Back in 2007, the company showed off a machine which was certainly a computer - it calculated a seating plan and completed a Sudoku puzzle - but which many doubted was actually relying on quantum effects to work.

Rather than the simple on/off switch of standard computers, quantum computing relies on quantum bits, or qubits, which can be both on and off simultaneously, making for massively parallel computing.

But while many scientists have demonstrated this on a small scale in the lab, there's been much doubt raised over whether D-Wave had really been able to create, as claimed, a working 128-qubit computer.

Many experts suspected that its machine was instead relying on classical physics for its effects.

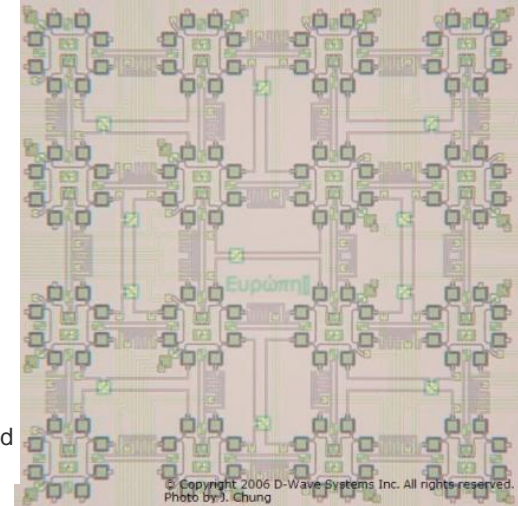
However, a recent paper in *Nature* appeared to back up its claims - and seems to have been enough to convince Lockheed Martin. It's signed a multi-year contract for the system, maintenance and support, and plans to use it for some of its most challenging computation problems, says D-Wave.

D-Wave says the machine is ideal for software verification and validation, financial risk analysis, affinity mapping and sentiment analysis and object recognition in images.

"D-Wave is thrilled to establish a strategic relationship with Lockheed Martin Corporation," says Vern Brownell, D-Wave's president and CEO.

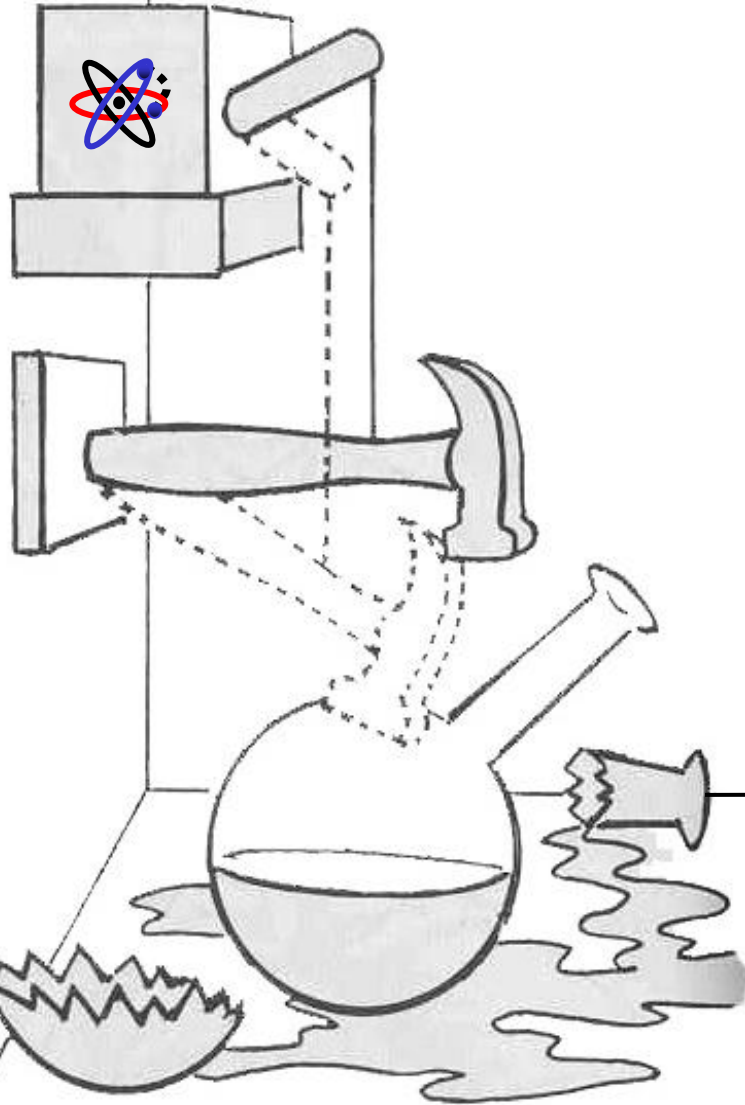
"Our combined strength will provide capacity for innovation needed to tackle important unresolved computational problems of today and tomorrow. Our relationship will allow us to significantly advance the potential of quantum computing."

In other words, Lockheed Martin will act as a sort of testing ground for D-Wave, perhaps making the whole deal more of a joint development partnership, rather than a straightforward sale. Still, it shows that Lockheed Martin believes that D-Wave is really onto something.

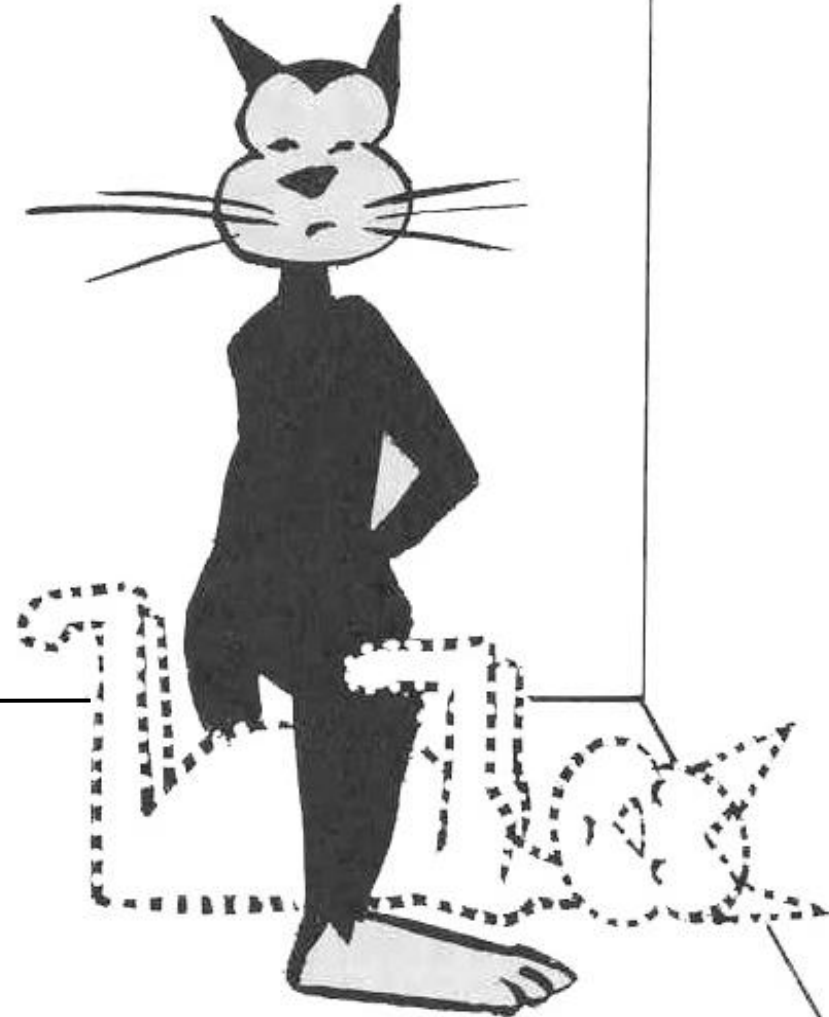


CAN THE CAT BE ALIVE AND
DEAD AT THE SAME TIME?

$N=1$



$N=10^{28}$



Richard Feynman (1982)



We have always had a great deal of difficulty in understanding the world view that quantum mechanics represents...

...Okay, I still get nervous with it...

It has not yet become obvious to me that there is no real problem. I cannot define the real problem, therefore I suspect there's no real problem, but I'm not sure there's no real problem.

Number cruncher turns 50

1st electronic computer feted

By Michael Raphael
The Associated Press

PHILADELPHIA — It had no monitor, could remember only 20 numbers at a time, and filled a room with 50 tons of electricity-sucking gear.

But it could crunch numbers with what seemed like blinding speed.

Fifty years ago this week, the Electronic Numerical Integrator and Computer was demonstrated for the first time at the University of Pennsylvania.

ENIAC counted to 5,000 in one-fifth of a second, shocking the world out of the mechanical age and into the world of lightning-quick digital processing.

ENIAC's collection of 8-foot-high gray cabinets made up the first general-purpose, large-scale, electronic computer.

Until then, "computers" were people using mechanical calculators who needed 12 hours to do what ENIAC did in half a minute. Other electronic machines had been narrower in purpose.

Monday, February 12, 1996

THE DENVER POST

7

Granddaddy of computers turning 50

COMPUTERS from Page 1A

"Without it, we wouldn't have the space program, we wouldn't have modern airplanes," said Michael Williams, editor in chief of the *Annals of the History of Computing*. "Pilots would still be trying to fly by looking outside the window occasionally."

ENIAC long ago outgrew its usefulness as a number cruncher — a \$40 calculator has more computing power.

But it has not lost its relevance.

The university planned an entire year of events to honor ENIAC's birthday, including turning on part of the original machine. Vice President Al Gore will throw a switch Wednesday, the day of the anniversary, and ENIAC will count from 46 to 96.

The Postal Service will unveil a stamp commemorating "The Birth of Computing." And Garry Kasparov, the World Chess Federation champion, this week is playing against IBM's "Deep Blue" computer.

The original assemblage of wires, vacuum tubes, resistors and switches was constructed in about a year and a half at the university's Moore School of Electrical Engineering.

When fully operational, ENIAC filled up a 30-by-50-foot room. Every second it was on, it used enough electricity — 174 kilowatts — to power a typical Philadelphia home for 1½ weeks.

Costing more than \$486,000, ENIAC might never been attempted



Associated Press

CALCULATING MINDS: J. Presper Eckert, masterminded ENIAC, pictured in undated photo left foreground, and John Mauchly, near pole, from the University of Pennsylvania Archives.

were it not for World War II.

"A lot of people said we were dreaming," said Herman Goldstine, who served as liaison between the Army and ENIAC team.

"The electronics people said there were too many vacuum tubes and it would never run. The mathematics people said there were no problems complex enough that computers were needed."

The Army provided both the complex problems and the money.

John Mauchly, one of two masterminds behind ENIAC, knew the Army was having a terrible time working out the complicated firing tables to help gun crews aim new artillery being used against German forces.

Each firing table had to list numbers for hundreds of potential trajectories. Calculating a single trajectory could take 40 hours using a mechanical desktop calculator, and 30 minutes using a sophisticated machine called a differential analyzer.

Mauchly, then 32, bravely told Army officials his machine could do the job in a matter of minutes.

ENIAC was completed just as the war was ending, too late for those artillery tables.

However, it fulfilled another military purpose. During test runs in 1944 it did millions of calculations on thermonuclear chain reactions, predicting the destruction that could be caused by the hydrogen bomb.